#3

Docket No. 1614.1085/HJS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Syuichi SATAKE

Group Art Unit:

Serial No.:

Examiner:

Filed: October 11, 2000

For: APPARATUS AND METHOD FOR AUTHENTICATING DIGITAL SIGNATURES AND COMPUTER-READABLE RECORDING MEDIUM THEREOF

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application(s):

Japanese Patent Application No. 11-332984
Filed: November 24, 1999

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: October 11, 2000

By: _____

H. J. Staas
Registration No. 22,010

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

#3

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年１１月２４日

出 願 番 号
Application Number: 平成１１年特許願第３３２９８４号

出 願 人
Applicant (s): 富士通株式会社

２０００年 ５月１９日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３０３６７５６

【書類名】　特許願

【整理番号】　9950595

【提出日】　平成11年11月24日

【あて先】　特許庁長官　近藤　隆彦　殿

【国際特許分類】　G06F 16/00

【発明の名称】　認証装置、認証方法及びその装置での処理をコンピュータに行なわせるためのプログラムを格納した記憶媒体

【請求項の数】　9

【発明者】

【住所又は居所】　富山県婦負郡八尾町保内二丁目２番１　株式会社富山富士通内

【氏名】　佐竹　修一

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100070150

【郵便番号】　150

【住所又は居所】　東京都渋谷区恵比寿４丁目２０番３号　恵比寿ガーデンプレイスタワー３２階

【弁理士】

【氏名又は名称】　伊東　忠彦

【電話番号】　03-5424-2511

【手数料の表示】

【予納台帳番号】　002989

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9704678

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　認証装置、認証方法及びその装置での処理をコンピュータに行なわせるためのプログラムを格納した記憶媒体

【特許請求の範囲】

【請求項１】　デジタル署名を認証する認証装置において、

署名者が設定した秘密鍵とデジタル文書の改ざんをチェックするダイジェスト情報とで暗号化してデジタル署名を生成する署名生成手段と、

該デジタル署名と所定のマークとを合成したイメージ情報を作成する署名組み込み手段と、

該署名組み込み手段で作成されたイメージ情報を、該デジタル文書内の指定された位置に埋め込むイメージ埋め込み手段とを有する認証装置。

【請求項２】　請求項１記載の認証装置において、

上記署名組み込み手段は、第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、所定のマークに対応したピクセルに対して第一の指定情報を設定し、他のピクセルに対してデジタル署名を構成する数列の各数値に対応した指定情報を設定することにより、イメージ情報としてのピクセルデータを生成するイメージ情報生成手段とを有するようにした認証装置。

【請求項３】　請求項２記載の認証装置において、

上記イメージ情報生成手段は、先頭のピクセルから順次、所定のマークに対応したピクセルをスキップしながら、デジタル署名を構成する数列の先頭から各数値に対応した指定情報を各ピクセルに設定するようにした認証装置。

【請求項４】　デジタル署名を認証する認証装置において、

デジタル文書内に埋め込まれたイメージ情報からデジタル署名を分離する署名分離手段と、

署名者によって公開された公開鍵で該デジタル署名を復号化して該デジタル文書の改ざんをチェックする第一のダイジェスト情報を獲得するダイジェスト獲得手段と、

該デジタル文書から再生する第二のダイジェスト情報と、ダイジェスト獲得手

段によって獲得された該第一のダイジェスト情報とが一致するかを判定し、一致した場合のみ該デジタル署名を認証する認証手段とを有する認証装置。

【請求項５】　請求項４記載の認証装置において、

上記署名分離手段は、第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、イメージ情報を構成するピクセルデータから第一の指定情報を取り除いたピクセルデータをデジタル署名とすることによってデジタル署名を再生するようにした認証装置。

【請求項６】　デジタル署名を認証する認証方法において、

署名者が設定した秘密鍵とデジタル文書の改ざんをチェックするダイジェスト情報とで暗号化して該デジタル署名を生成する署名生成手順と、

第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、所定のマークに対応したピクセルに対して第一の指定情報を設定し、他のピクセルに対してデジタル署名を構成する数列の各数値に対応した指定情報を設定することにより、イメージ情報としてのピクセルデータを生成するイメージ情報生成手順と、

該イメージ情報手順で作成されたイメージ情報を、該デジタル文書内の指定された位置に埋め込むイメージ埋め込み手順とを有する認証方法。

【請求項７】　デジタル署名を認証する認証方法において、

第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、イメージ情報を構成するピクセルデータから第一の指定情報を取り除いたピクセルデータをデジタル署名とすることによってデジタル署名を再生する署名再生手順と、

署名者によって公開された公開鍵で、該署名再生手順で再生された該デジタル署名を復号化して該デジタル文書の改ざんをチェックする第一のダイジェスト情報を獲得するダイジェスト獲得手順と、

該デジタル文書から再生する第二のダイジェスト情報と、該ダイジェスト獲得手順によって獲得された該第一のダイジェスト情報とが一致するかを判定し、一致した場合のみ該デジタル署名を認証する認証手順とを有する認証方法。

【請求項８】　デジタル署名を認証する認証装置での処理をコンピュータに行なわせるためのプログラムを格納した記憶媒体において、

署名者が設定した秘密鍵とデジタル文書の改ざんをチェックするダイジェスト情報とで暗号化して該デジタル署名を生成する署名生成手順と、

第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、所定のマークに対応したピクセルに対して第一の指定情報を設定し、他のピクセルに対してデジタル署名を構成する数列の各数値に対応した指定情報を設定することにより、イメージ情報としてのピクセルデータを生成するイメージ情報生成手順と、

該イメージ情報手順で作成されたイメージ情報を、該デジタル文書内の指定された位置に埋め込むイメージ埋め込み手順とを有するプログラムを格納した記憶媒体。

【請求項９】　デジタル署名を認証する認証装置での処理をコンピュータに行なわせるためのプログラムを格納した記憶媒体において、

第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、イメージ情報を構成するピクセルデータから第一の指定情報を取り除いたピクセルデータをデジタル署名とすることによってデジタル署名を再生する署名再生手順と、

署名者によって公開された公開鍵で、該署名再生手順で再生された該デジタル署名を復号化して該デジタル文書の改ざんをチェックする第一のダイジェスト情報を獲得するダイジェスト獲得手順と、

該デジタル文書から再生する第二のダイジェスト情報と、該ダイジェスト獲得手順によって獲得された該第一のダイジェスト情報とが一致するかを判定し、一致した場合のみ該デジタル署名を認証する認証手順とを有するプログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル文書を認証する認証装置に係り、詳しくは、デジタル文章

の認証に用いるランダムな数又は文字の列からなるデジタル署名を署名者の署名マークと共にイメージ情報に組み込むことにより視認性を向上するようにした認証装置を提供するものである。

【０００２】

また、本発明は、そのような認証方法及びその装置での処理をコンピュータに行なわせるためのプログラムを格納した記憶媒体に関する。

【０００３】

【従来の技術】

図１に示されるようなクライアント／サーバのネットワークにおいて、複数のクライアントとサーバがネットワークを介して接続されている。このようなネットワークシステムにおいて、決裁業務をグループウェアを利用して電子的に行なう電子決裁システムが広く知られている。

【０００４】

電子決裁システムでは、デジタル署名が使用されている。例えば、図１より、クライアントＡの利用者Ａが作成した文書にデジタル署名を添付しクライアントＢの利用者Ｂへその文書を送信する。クライアントＢの利用者Ｂは、クライアントＡの利用者Ａのデジタル署名を解読するための公開鍵を取得し、その公開鍵を使用して受信した文書に添付されたデジタル署名を解読する。解読が成功すれば、その文書は、確かにクライアントＡの利用者Ａから送信されたものであり、かつ、文書の改ざんがされなかったことを示す。このように、デジタル署名を使用することで文書作成者（送信者）の認証が可能となり、作成したデジタル文書を紙に印刷しその紙文書への文書作成者の押印を不要とすることができた。

【０００５】

【発明が解決しようとする課題】

しかしながら、上記従来におけるデジタル署名においては、以下に述べる問題点がある。

先ず、デジタル署名は、ランダムな意味のない数又は文字の列で構成されるため、紙文書の押印であれば瞬時に文書作成者の押印であるかの判断ができるような視覚的な効果がない。そのため、デジタル署名が添付されたデジタル文書の受

信者は、送信者のいつものデジタル署名との相違を区別できないため、意味のない数又は文字の列を見せられる煩わしさを感じると同時に、デジタル署名の解読の手間による煩わしさを感じる場合がある。

【０００６】

さらに、近年におけるデジタル署名は、５１２ビットから１０２４ビット程の長さを要し、紙文書の押印に比べると、表示スペースを多く必要としている。

また、デジタル署名は、押印と異なり署名位置が文末に限られている。

そこで、本発明の第一の課題は、デジタル文章の認証に用いるランダムな数又は文字の列からなるデジタル署名を署名者の署名マークと共にイメージ情報に組み込むことにより視認性を向上するようにした認証装置を提供することである。

【０００７】

また、本発明の第二の課題は、同様に、デジタル文章の認証に用いるランダムな数又は文字の列からなるデジタル署名を署名者の署名マークと共にイメージ情報に組み込み視認性を向上するようにした認証方法を提供することである。

さらに、本発明の第三の課題は、上記のような認証装置での処理をコンピュータに行なわせるためのプログラムを格納した記憶媒体を提供することである。

【０００８】

【課題を解決するための手段】

上記第一の課題を解決するため、本発明は、請求項１記載に記載されるように、デジタル署名を認証する認証装置において、署名者が設定した秘密鍵とデジタル文書の改ざんをチェックするダイジェスト情報とで暗号化してデジタル署名を生成する署名生成手段と、該デジタル署名と所定のマークとを合成したイメージ情報を作成する署名組み込み手段と、該署名組み込み手段で作成されたイメージ情報を、該デジタル文書内の指定された位置に埋め込むイメージ埋め込み手段とを有するように構成される。

【０００９】

このような認証装置では、署名者を認証するための秘密鍵とデジタル文書の改ざんをチェックするダイジェスト情報とが暗号化されてデジタル署名が作成される。そして、そのデジタル署名はイメージ情報に組み込まれ、さらに、デジタル

文書に埋め込まれる。

従って、ネットワークを介してデジタル署名を含むデジタル文書を受け取る受信者は、署名者から送られたことをイメージ情報で表現されるマークによって受信者の目で確認することができる。また、デジタル署名により、受信者に対し、署名者本人であることの証明とデジタル文書の改ざん防止の両方を同時に証明することができる。

【００１０】

上記秘密鍵は、署名者が独自に設定するものでどんな数又は文字の列が設定可能である。

上記ダイジェスト情報は、デジタル文書の改ざんを防止するために、デジタル文書のデータと所定の計算方法によって導き出されるデータであり、例えば、ＭＤ(Message Digest)ファイルを作成するツールを利用することによって得られる。

【００１１】

上記マークは、署名者が押印した印鑑等の印影又は署名者直筆のサインなどである。

上記イメージ情報は、署名者を判別するのに相応しい上記マークをデジタル化したイメージ情報であれば良い。例えば、署名者の名前や日付入りの印鑑を模した図をペイントツール等で作成したイメージ、署名者直筆のサインをスキャナで読み込んで作成したイメージ、タブレットで作成したサイン、或いは、署名者が押印した印影をスキャナで読み込んで作成したイメージ等である。

【００１２】

デジタル署名がイメージ情報に組み込むことができるという観点から、本発明は、請求項２に記載されるように、上記署名組み込み手段は、第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、所定のマークに対応したピクセルに対して第一の指定情報を設定し、他のピクセルに対してデジタル署名を構成する数列の各数値に対応した指定情報を設定することにより、イメージ情報としてのピクセルデータを生成するイメージ情報生成手段とを有するように構成することができる。

【００１３】

このような認証装置では、イメージ情報を構成するピクセルデータがデジタル署名を構成する数列に置き換えられる。従って、冗長したデジタル署名が文書内に記述されることがない。かつ、デジタル署名をピクセルデータに組み込むことで、表示領域を大幅に縮小することができる。さらに、文書のいかなる場所にも表示できる。

【００１４】

また、このような認証装置では、例えば、第一の指定情報は、パレットの第一番目を指定し第一の色情報が設定され、パレットの二番目以降にはすべて同じ色の第二の色情報が設定される。従って、パレットの第一番目に「黒」又は「赤」を示す第一の色情報を指定し、パレットの第二番目以降には全て「白」を示す第二の色情報を指定した場合、デジタル署名を組み込んだピクセルデータを表示した際に、署名部分（マーク）は「黒」又は「赤」で表示され、デジタル署名の数値列部分は「白」で表示されるので、署名者が作成したマークが変形することがない。つまり、第一の色情報と第二の色情報は、互いに異なる色を表わす情報であれば良く、上記の色の設定に限定されない。

【００１５】

また、デジタル署名を構成する数列をイメージ情報の他の指定情報に対応させるという観点から、本発明は、請求項３に記載されるように、上記イメージ情報生成手段は、先頭のピクセルから順次、所定のマークに対応したピクセルをスキップしながら、デジタル署名を構成する数列の先頭から各数値に対応した指定情報を各ピクセルに設定するように構成される。

【００１６】

上記第一の課題を解決するために、さらに、本発明は、請求項４に記載されるように、デジタル署名を認証する認証装置において、デジタル文書内に埋め込まれたイメージ情報からデジタル署名を分離する署名分離手段と、署名者によって公開された公開鍵で該デジタル署名を復号化して該デジタル文書の改ざんをチェックする第一のダイジェスト情報を獲得するダイジェスト獲得手段と、該デジタル文書から再生する第二のダイジェスト情報と、ダイジェスト獲得手段によって

獲得された該第一のダイジェスト情報とが一致するかを判定し、一致した場合のみ該デジタル署名を認証する認証手段とを有するように構成される。

【００１７】

このような認証装置は、復号化により獲得した第一のダイジェスト情報と、デジタル文書から再生した第二のダイジェスト情報を比較することによってデジタル署名の認証を行なう。

従って、比較結果が一致する場合に、署名者本人であることの証明とデジタル文書の改ざんが行なわれなかったことの両方を同時に証明することができる。

【００１８】

イメージ情報に組み込まれたデジタル署名を分離するという観点から、本発明は、請求項５に記載されるように、請求項４記載の認証装置において、上記署名分離手段は、第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、イメージ情報を構成するピクセルデータから第一の指定情報を取り除いたピクセルデータをデジタル署名とすることによってデジタル署名を再生するように構成することができる。

【００１９】

上記第二の課題を解決するため、本発明は、請求項６に記載されるように、デジタル署名を認証する認証方法において、デジタル署名を認証する認証方法において、署名者が設定した秘密鍵とデジタル文書の改ざんをチェックするダイジェスト情報とで暗号化して該デジタル署名を生成する署名生成手順と、第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、所定のマークに対応したピクセルに対して第一の指定情報を設定し、他のピクセルに対してデジタル署名を構成する数列の各数値に対応した指定情報を設定することにより、イメージ情報としてのピクセルデータを生成するイメージ情報生成手順と、該イメージ情報手順で作成されたイメージ情報を、該デジタル文書内の指定された位置に埋め込むイメージ埋め込み手順とを有するように構成される。

【００２０】

上記第二の課題を解決するため、さらに、本発明は、請求項７に記載されるように、デジタル署名を認証する認証方法において、デジタル署名を認証する認証方法において、第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、イメージ情報を構成するピクセルデータから第一の指定情報を取り除いたピクセルデータをデジタル署名とすることによってデジタル署名を再生する署名再生手順と、署名者によって公開された公開鍵で、該署名再生手順で再生された該デジタル署名を復号化して該デジタル文書の改ざんをチェックする第一のダイジェスト情報を獲得するダイジェスト獲得手順と、該デジタル文書から再生する第二のダイジェスト情報と、該ダイジェスト獲得手順によって獲得された該第一のダイジェスト情報とが一致するかを判定し、一致した場合のみ該デジタル署名を認証する認証手順とを有するように構成される。

【００２１】

上記第三の課題を解決するため、本発明は、請求項８に記載されるように、デジタル署名を認証する認証装置での処理をコンピュータに行なわせるためのプログラムを格納した記憶媒体において、署名者が設定した秘密鍵とデジタル文書の改ざんをチェックするダイジェスト情報とで暗号化して該デジタル署名を生成する署名生成手順と、第一の指定情報に対して第一の色情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、所定のマークに対応したピクセルに対して第一の指定情報を設定し、他のピクセルに対してデジタル署名を構成する数列の各数値に対応した指定情報を設定することにより、イメージ情報としてのピクセルデータを生成するイメージ情報生成手順と、該イメージ情報手順で作成されたイメージ情報を、該デジタル文書内の指定された位置に埋め込むイメージ埋め込み手順とを有するプログラムを格納した記憶媒体として構成される。

【００２２】

上記第三の課題を解決するため、さらに、本発明は、請求項９に記載されるように、デジタル署名を認証する認証装置での処理をコンピュータに行なわせるためのプログラムを格納した記憶媒体において、第一の指定情報に対して第一の色

情報が設定されると共に、他の指定情報に対して第二の色情報が設定されたパレットを参照して、イメージ情報を構成するピクセルデータから第一の指定情報を取り除いたピクセルデータをデジタル署名とすることによってデジタル署名を再生する署名再生手順と、署名者によって公開された公開鍵で、該署名再生手順で再生された該デジタル署名を復号化して該デジタル文書の改ざんをチェックする第一のダイジェスト情報を獲得するダイジェスト獲得手順と、該デジタル文書から再生する第二のダイジェスト情報と、該ダイジェスト獲得手順によって獲得された該第一のダイジェスト情報とが一致するかを判定し、一致した場合のみ該デジタル署名を認証する認証手順とを有するプログラムを格納した記憶媒体として構成される。

【００２３】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。

本発明の実施の一形態に係る認証端末が構成されるコンピュータシステムのハードウェア構成は、例えば、図２に示すようになっている。

図２において、このシステムは、ＣＰＵ（中央演算処理ユニット）１１、メモリユニット１２、通信ユニット１３、入力ユニット１４、表示ユニット１５、補助記憶装置１６及びＣＤ－ＲＯＭドライブユニット１７を有している。これらの各ユニット１１、１２、１３、１４、１５、１６及びＣＤ－ＲＯＭドライブユニット１７は、バスＢに接続されている。

【００２４】

ＣＰＵ１１は、メモリユニット１２に格納されたプログラムに従って当該認証端末を制御すると共に、後述するような認証端末での処理を行う。メモリユニット１２は、ＲＡＭ及びＲＯＭにて構成され、ＣＰＵ１１にて実行されるプログラム、ＣＰＵ１１での処理に必要なデータ、ＣＰＵ１１での処理にて得られたデータ等を格納する。また、メモリユニット１２の一部の領域が、ＣＰＵ１１での処理に利用されるワークエリアとして割り付けられている。

【００２５】

入力ユニット１４は、マウス、キーボード等を有し、利用者が後述するような

認証処理を行なうための登録や登録したデータの変更等、必要な各種情報を入力するために用いられる。表示ユニット１６は、ＣＰＵ１１の制御のもとに利用者に必要な各種情報を表示する。

補助記憶装置１６は、例えば、ハードディスクユニットにて構成され、各種ファイル、プログラムを格納する。

【００２６】

認証処理に係るプログラムは、例えば、ＣＤ－ＲＯＭ５０によって当該装置に提供される。即ち、認証処理に係るプログラムが保存されたＣＤ－ＲＯＭ５０がＣＤ－ＲＯＭドライブユニット１７にセットされると、ＣＤ－ＲＯＭドライブユニット１７がＣＤ－ＲＯＭ５０から当該プログラムを読み出し、その読み出されたプログラムがバスＢを介して補助記憶装置１６にインストールされる。そして、この認証処理が起動されると、補助記憶装置１６にインストールされた当該プログラムに従ってＣＰＵ１１がその処理を開始する。尚、当該プログラムを格納する媒体としてＣＤ－ＲＯＭ５０に限定するものではなく、コンピュータが読み取り可能な媒体であればよい。

【００２７】

本発明の実施の一形態に係る認証端末における検印情報の登録処理について、図３と図４で説明する。図３は、検印情報の登録処理を説明するフローチャート図である。図４は、検印情報を登録するための画面の例を示す図である。図４（Ａ）は、検印者情報の設定画面の例を示す図であり、図４（Ｂ）は、印鑑イメージの登録画面の例を示す図である。

【００２８】

図３において、秘密情報（パスワード等）及び公開情報（利用者の氏名又は役職等）などの検印者情報の登録を行なうため、クライアントＡの利用者Ａは表示ユニット１５に図４（Ａ）に示す検印者情報の設定画面４１を開き、利用者Ａの社員番号を社員番号の入力フィールドに入力し（ステップＳ１）、続けて、印鑑の名称（例えば、「日付印１」或いは「認印１」等）を印鑑名称の入力フィールドに入力し（ステップＳ２）登録ボタンをクリックする。すると、次に、図４（Ｂ）に示す印鑑イメージの登録画面４３が表示ユニット１５に現れる。印鑑イメ

ージの登録画面で、名前フィールドに名前を入力し（ステップＳ３）、役職フィールドに役職名を入力する（ステップＳ４）。さらに、印鑑形状の選択フィールドから形状を選択し（ステップＳ５）、印鑑サイズフィールドに印鑑サイズを、例えば、ミリ（ｍｍ）単位で指定する（ステップＳ６）。例えば、利用者Ａが名前に「富士」を、役職に「開発課長」を、印鑑形状に「丸（日付有り）」を、印鑑サイズに「１２」ｍｍを設定し登録すると、印鑑イメージ表示領域４５に上記指定に応じた印鑑イメージが作成され表示される（ステップＳ７）。登録ボタンをクリックし印鑑イメージを登録する。上記入力値と作成された印鑑イメージが補助記憶装置１６へ登録される。

【００２９】

印鑑イメージは、スキャナーを用いて読み込んで作成し補助記憶装置１６に登録しても良い。例えば、利用者Ａのサインなどをスキャナで読み込んで電子化したサインを印鑑イメージとして補助記憶装置１６に登録しても良い。印鑑イメージがドロー（ベクトル）情報である場合にはスキャナは不要である。

以上により、図４（Ａ）の検印者情報の設定画面４１及び図４（Ｂ）の印鑑イメージの登録画面４３の画面上から利用者Ａにより入力された公開情報（利用者の社員番号、名前、役職など）、印鑑名称、及び、印鑑イメージ情報（印鑑形状、印鑑サイズなど）は、補助記憶装置１６に登録される。

【００３０】

次に、利用者Ａは、作成した文書に登録された検印を埋め込む。

文書内に埋め込む検印の実行処理について、図５及び図６で説明する。図５は、検印の実行処理を説明するフローチャート図である。図６は、検印を実行する画面の例を示す図である。図６（Ａ）は、作成した文書上に開かれた検印実行画面の例を示す図である。図６（Ｂ）は、作成した文書上に開かれた検印実行通知画面の例を示す図である。

【００３１】

図５において、利用者Ａは、作成した文章（検印文書）上に、検印実行画面６１を開き、予め登録しておいた印鑑を埋め込む領域６３を文章上で指定する（ステップＳ１１）。また、検印実行画面の社員番号フィールドに利用者の所定の社

員番号を、印鑑フィールドに利用者の所定の印鑑名称を、秘密鍵フィールドに利用者の秘密鍵を各々入力し、確認ボタンをクリックする（ステップＳ１２）。利用者Ａによる確認ボタンのクリックにより、クライアントＡのＣＰＵ１１は、作成した文書（検印文書）の内容を保証するＭＤ（Message Digest）ファイル（ダイジェスト情報）を作成する（ステップＳ１３）。さらに、作成したダイジェスト情報を暗号化する（ステップＳ１４）。デジタル署名は、利用者が入力した秘密鍵にてダイジェスト情報を所定の方法で暗号化することによって作成される。

【００３２】

一方、社員番号及び印鑑名称から、登録されている印鑑イメージデータを検索して獲得する。

これにより、クライアントＡは、獲得したイメージ情報から検印用の印鑑イメージを再生する（ステップＳ１５）。再生した印鑑イメージ内に上記作成したデジタル署名を組み込む（ステップＳ１６）。デジタル署名を印鑑イメージに組み込む方法は後述する。デジタル署名が組み込まれた印鑑イメージは、検印実行画面６１で指定した検印文書の領域６３に埋め込まれ、図６（Ｂ）に示す検印実行通知画面６５が表示される（ステップＳ１７）。利用者Ａが確認ボタンをクリックすることにより、検印文書への埋め込みが確認され処理が終了する。

【００３３】

上述のように、デジタル署名が印鑑イメージと共にＨＴＭＬ、ＳＧＭＬ、ＸＭＬ等の文書に組み込まれ、ネットワークを介して別のクライアントＢへ送信される。

次に、デジタル署名が印鑑イメージと共に組み込まれた文章を受信した場合の検証処理について図７、図８及び図９で説明する。図７は、印鑑イメージの検証処理を説明するフローチャート図である。また、図８（Ａ）は、検印の確認実行画面を示す図であり、図８（Ｂ）は、検印が正当の場合の確認画面を示す図である。さらに、図９は、検印が不正の場合の確認画面を示す図である。

【００３４】

受信側利用者のクライアントも図２に示すハードウェア構成を有するものとする。

図７において、受信側利用者Ｂは、クライアントＢの表示ユニット１５で受信した文書内の検証する検印位置８３を指定し、図８（Ａ）に示す検印の確認実行画面８１を開く（ステップＳ４１）。続いて、利用者Ｂは、公開鍵を取得する（ステップＳ４２）。例えば、サーバがインターネット上等で公開している公開鍵リストから、送信者の名前又は社員番号等で検索し該当する公開鍵を取得する。取得した公開鍵を図８（Ａ）の検印の確認実行画面８１上の公開鍵フィールドに入力し、確認ボタンをクリックする。

【００３５】

クライアントＢのＣＰＵ１１は、指定された検印位置８３の印鑑イメージの全体から印鑑イメージを取り除き、デジタル署名を取得する（ステップＳ４３）。

次に、取得した公開鍵でデジタル署名を復号化する。デジタル署名は、ダイジェスト情報と秘密鍵で暗号化されているので、この復号化により、組み込まれたダイジェスト情報が取り出される（ステップＳ４４）。

【００３６】

さらに、受信した文章のＭＤファイル（ダイジェスト情報）を作成する（ステップＳ４５）。受信文書のダイジェスト情報と復号化で取り出されたダイジェスト情報を比較し（ステップＳ４６）、比較結果を利用者Ｂに通知する（ステップＳ４７）。両方のダイジェスト情報が互いに一致する場合は、表示ユニット１５に図８（Ｂ）に示される検印の確認画面８５が表示され、正当な検印であることが利用者に通知される。つまり、ステップＳ４４で正当なダイジェスト情報を獲得したことを意味し、本人認証が完了していたことを示す。また、ダイジェスト情報が一致しているので、文章が改ざんされていないことも証明する。一方、両方のダイジェスト情報が互いに一致しない場合は、表示ユニット１５に図９に示される検印の確認画面９１が表示され、不当な検印であることが通知される。本人認証が不正であったか、文章が改ざんされたかを意味する。または、本人認証も文章も共に不正であることを意味する。比較結果通知後、処理は終了する。

【００３７】

次に、前述のデジタル署名の印鑑イメージへの組み込み方法について図１０で詳細に説明する

送信側クライアントＡにおいて、ＣＰＵ１１は、図６（Ａ）に示す検印実行画面６１で利用者が入力した秘密鍵を（ステップＳ１２）取得し、作成された検印文書のダイジェスト情報（ステップＳ１３）とで、暗号化する関数等を使用し、図１０（Ａ）に示されるようなデジタル署名を生成する。図１０（Ａ）では、便宜上、１６進で表示する。

【００３８】

次に、作成された検印用の印鑑イメージ（ステップＳ１５）を取得する。印鑑イメージはピクセルデータ（ビットマップデータ）で構成され、ピクセルデータはパレットの位置を示すインデックス番号をピクセル毎に指定している。図６（Ｂ）に示す検印実行通知画面６５で検印が確認された文書上の検印領域６７は、例えば、その検印領域の背景色は白色で、検印（印鑑）の色（文字色）は黒色である。この場合、取得した印鑑イメージのピクセルデータは、黒色と白色を示す複数のインデックス番号の列で構成される。ＣＰＵ１１は、ピクセルデータの先頭から文字色以外を示す（白色を示す）インデックス番号をデジタル署名のデータに置き換える。例えば、印鑑イメージを作成する際に、印鑑の色（文字色）を常にパレットの先頭に指定するようにすれば、黒色のインデックス番号は「００（１６進）」であるので、「００」をスキップして、先頭から順番にデータを置き換える。ピクセルデータを含む印鑑イメージのヘッダ部（図示せず）に、イメージの全データの長さ、デジタル署名の長さ（つまり、黒色を省いたイメージの長さ）等の情報が付加される。

【００３９】

さらに、ＣＰＵ１１は２５６個のパレットを用意し、パレットの位置を示すインデックス番号「００（１６進）」から「ＦＦ（１６進）」の中で、黒色のインデックス番号で示されるパレット位置以外を白色を示す色データ（例えば、ＲＧＢデータ）に設定する。この場合、文字色は先頭に指定されるので、ＣＰＵ１１は、黒色を示すインデックス番号「００（１６進）」以外のインデックス番号「０１（１６進）」から「ＦＦ（１６進）」までのパレットを白色を示す色データに設定する。よって、図１０（Ｃ）に示される文字色が黒色で背景色が白色のパレットが作成される。これによって、暗号化され冗長したデジタル署名は、印鑑

イメージに組み込まれるため、意味のない冗長した文字列に煩わされることがない。また、印鑑イメージは変形されないので、利用者Ｂは容易に視認することができる。

【００４０】

上述によってデジタル署名が組み込まれた印鑑イメージが文書と共に送信され、他の利用者により受信される。受信した印鑑イメージの復号化について図１０（Ａ）及び図１０（Ｂ）で説明する。

受信側のクライアントＢにおいて、受信した文書内で確認検印の指定（ステップＳ４１）により取り出された印鑑イメージを構成するピクセルデータ（ビットマップデータ）が図１０（Ｂ）に示される。クライアントＢのＣＰＵ１１は、印鑑イメージのヘッダ部からイメージの全データの長さ、デジタル署名の長さ等の情報を取得する。この場合、文字色の指定はインデックス番号「００（１６進）」で指定されるので、ピクセルデータの「００（１６進）」をスキップしながら先頭から読み込むことにより、図１０（Ａ）に示されるデジタル署名を取り出すことができる（ステップＳ４３）。

【００４１】

次に、ＣＰＵ１１は、取り出されたデジタル署名を、取得した公開鍵（ステップＳ４１）と復号化関数等を使用することによって解読し、ダイジェスト情報を取得する（ステップＳ４４）。

上述の例では、公開鍵を利用者Ｂによってサーバから獲得するようにしているが、送信側のクライアントＡで印鑑イメージのヘッダ部に公開鍵を取得するための利用者Ａの名前又は社員番号等の情報を設定しても良い。この情報により、受信側のクライアントＢは利用者Ｂを介さずに自動的にサーバから公開鍵の獲得を行なうことができる。

【００４２】

また、背景部分にデジタル署名を組み込んであるが、印鑑の印影部分にデジタル署名を組み込んでも良い。この場合、図１０（Ｃ）において、インデックス番号「００（１６進）」で示される文字色の「黒」を背景色「白」とし、インデックス番号「０１（１６進）」から「ＦＦ（１６進）」までで示される背景色の「

白」を文字色の「黒」に設定することで可能となる。

【００４３】

上述によって、デジタル署名をイメージに組み込んでイメージ化することが可能である。つまり、ランダムな数又は文字列で表わされるデジタル署名がイメージ化されることで視認性を向上することができる。

また、イメージ化することで、５１２ビットから１０２４ビットの長さにもなる冗長したデジタル署名がピクセルデータに変換されるため、表示領域を小さくすることができる。

【００４４】

さらに、ＭＤファイル（ダイジェスト情報）と認証（パスワード）の組合せにより、文書の改ざん防止と本人認証とを同時にすることができる。

なお、上記例において、図５に示すステップＳ１３及びＳ１４での処理が請求項１の署名生成手段に対応し、図５に示すステップＳ１５及びＳ１６での処理が請求項１の署名組み込み手段に対応する。

【００４５】

また、図７に示すステップＳ４３での処理が請求項３の署名分離手段に対応し、図７に示すステップＳ４４での処理が請求項３のダイジェスト獲得手段に対応する。

【００４６】

【発明の効果】

以上、説明してきたように、請求項１乃至３記載の本願発明によれば、署名者を認証するための秘密鍵とデジタル文書の改ざんをチェックするダイジェスト情報とが暗号化されてデジタル署名が作成される。そして、そのデジタル署名は、イメージ情報に組み込まる。従って、ネットワークを介してデジタル署名を含むデジタル文書を受け取る受信者は、署名者から送られたことを署名マーク（印影等）によって受信者の目で確認することができ、また、デジタル署名により、受信者に対し、署名者本人であることの証明とデジタル文書の改ざん防止の両方を同時に証明することができる。

【００４７】

また、請求項４乃至５記載の本願発明によれば、イメージ情報に組み込まれた暗号化されたデジタル署名をイメージから分離し、復号化する。従って、イメージ情報によって署名者から送られた文書であることを確認すると共に、受け取ったデジタル文書が正当な文章であるかを判別することができる。

また、請求項６乃至７記載の本願発明によれば、デジタル文章の認証に用いるランダムな数列からなるデジタル署名を署名者の署名マークと共にイメージ情報に組み込み視認性を向上するようにした認証方法を提供することができる。

【００４８】

さらに、請求項７乃至８記載の本願発明によれば、上記のような認証装置での処理をコンピュータに行なわせるためのプログラムを格納した記憶媒体を提供することができる。

【図面の簡単な説明】

【図１】

クライアント／サーバのネットワーク概略図である。

【図２】

ハードウェア構成図である。

【図３】

検印情報の登録処理を説明するフローチャート図である。

【図４】

検印情報を登録するための画面の例を示す図である。

【図５】

検印の実行処理を説明するフローチャート図である。

【図６】

検印を実行する画面の例を示す図である。

【図７】

印鑑イメージの検証処理を説明するフローチャート図である。

【図８】

検印の確認する画面の例を示す図である。

【図９】

検印の確認する画面の例を示す図である。

【図１０】

デジタル署名のイメージ組み込み説明図である。

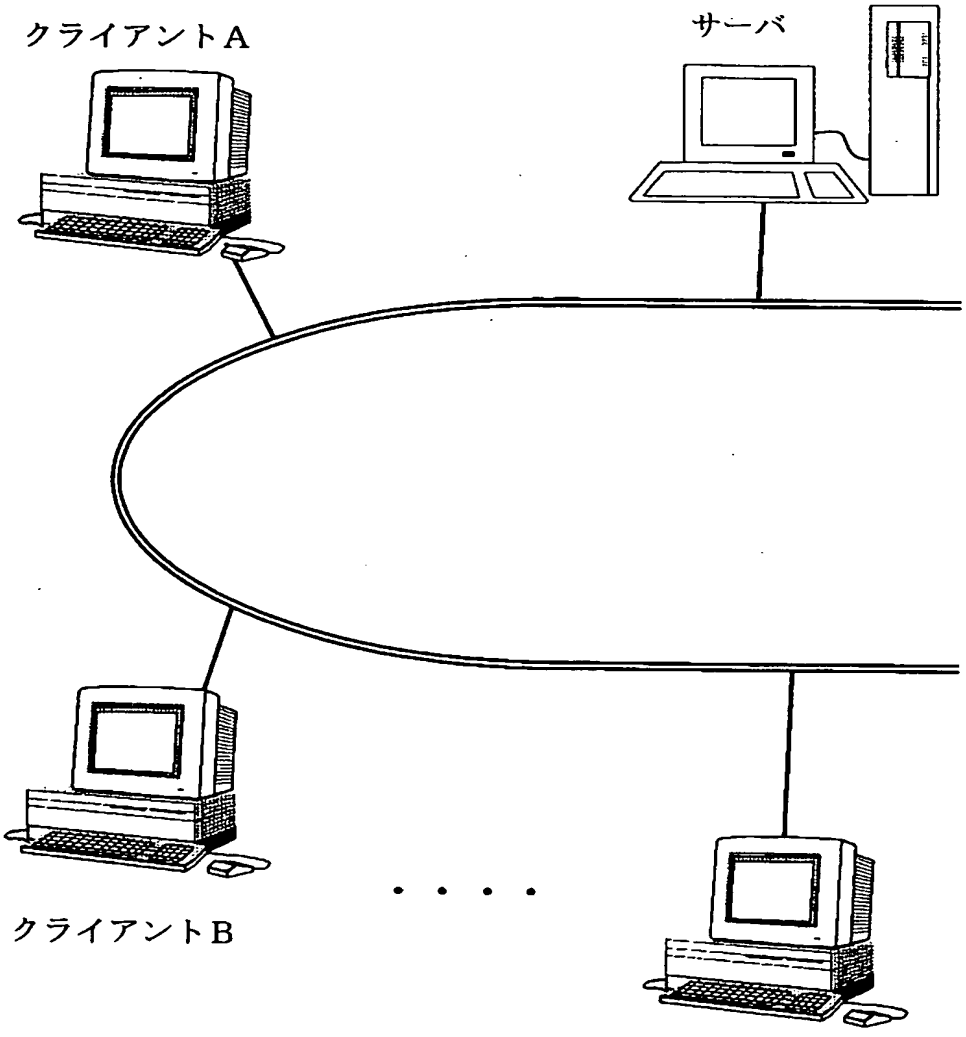
【符号の説明】

１１	ＣＰＵ
１２	メモリユニット
１３	通信ユニット
１４	入力ユニット
１５	表示ユニット
１６	補助記憶装置
１７	ＣＤ－ＲＯＭドライバ
５０	ＣＤ－ＲＯＭ
Ｂ	バス
４１	検印者情報の設定画面
４３	印鑑イメージの登録画面
６１	検印実行画面
６５	検印実行通知画面
８１	検印確認実行画面
８５	検印確認画面

【書類名】　図面

【図１】

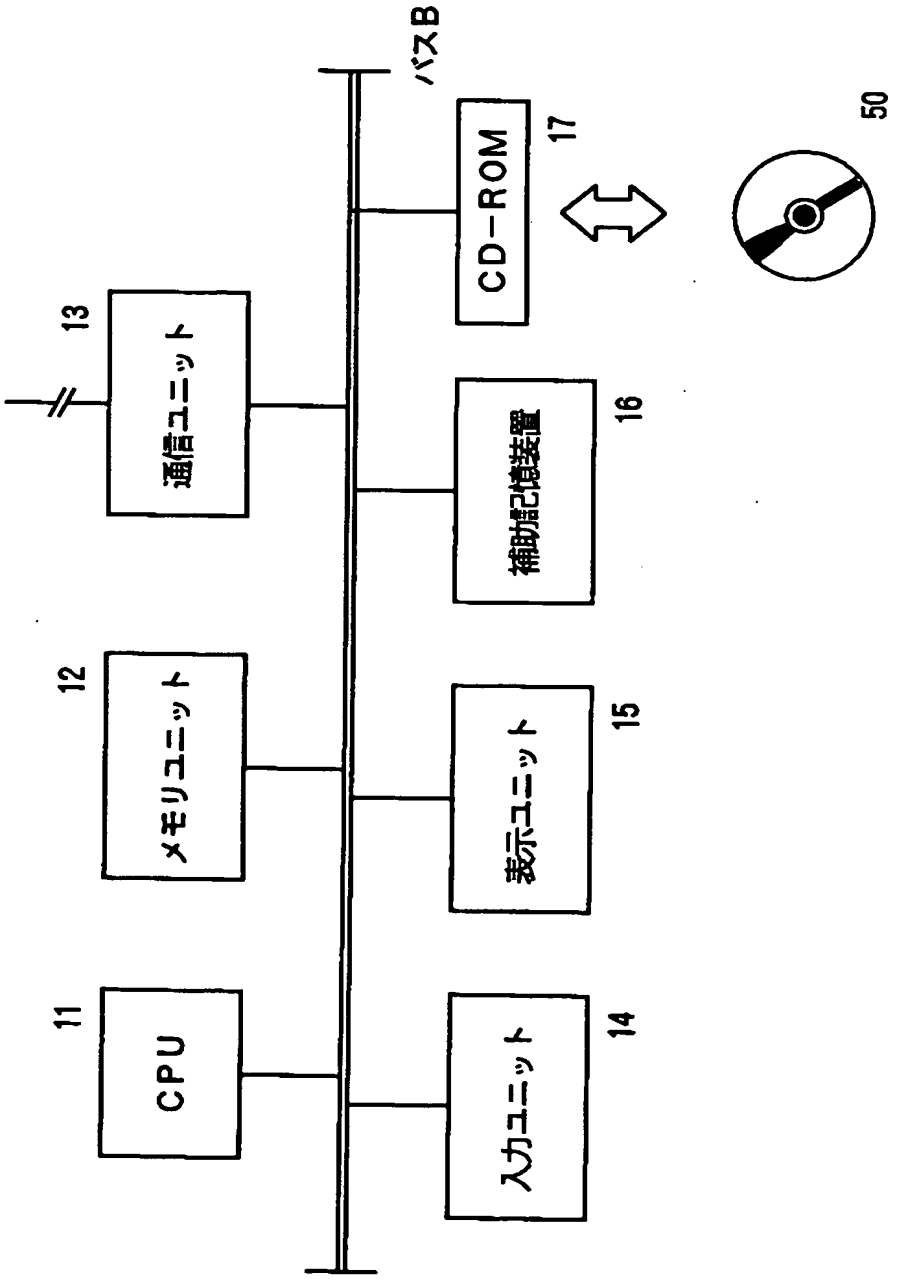
クライアント／サーバのネットワーク概略図



出証特２０００－３０３６７５６

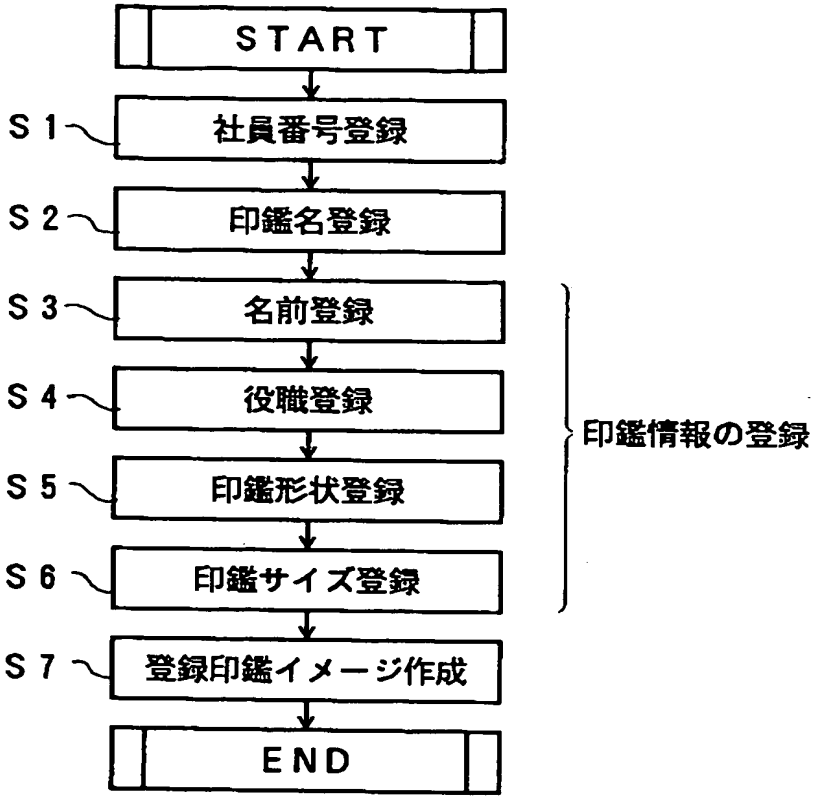
【図２】

ハードウェア構成図



【図３】

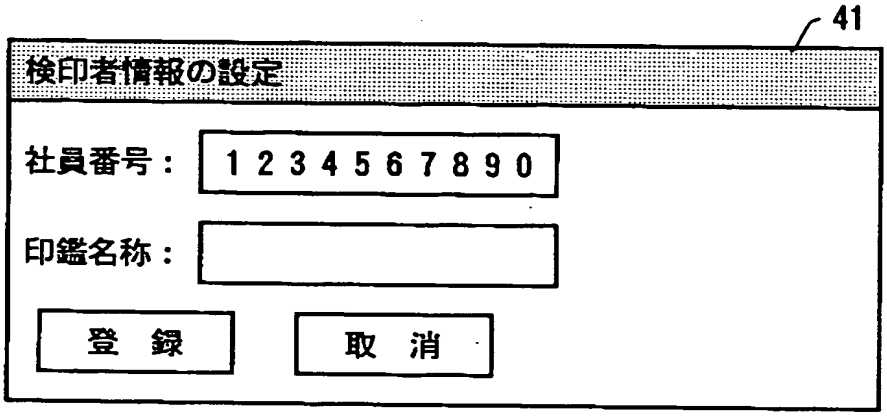
検印情報の登録処理を説明するフローチャート図



【図４】

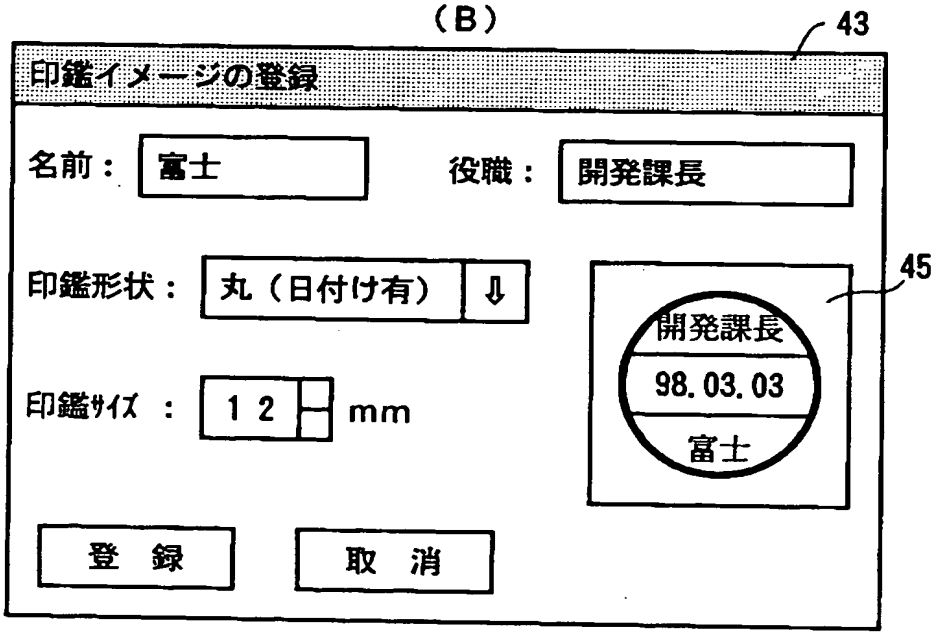
検印情報を登録するための画面の例を示す図

（A）



検印者情報の設定画面

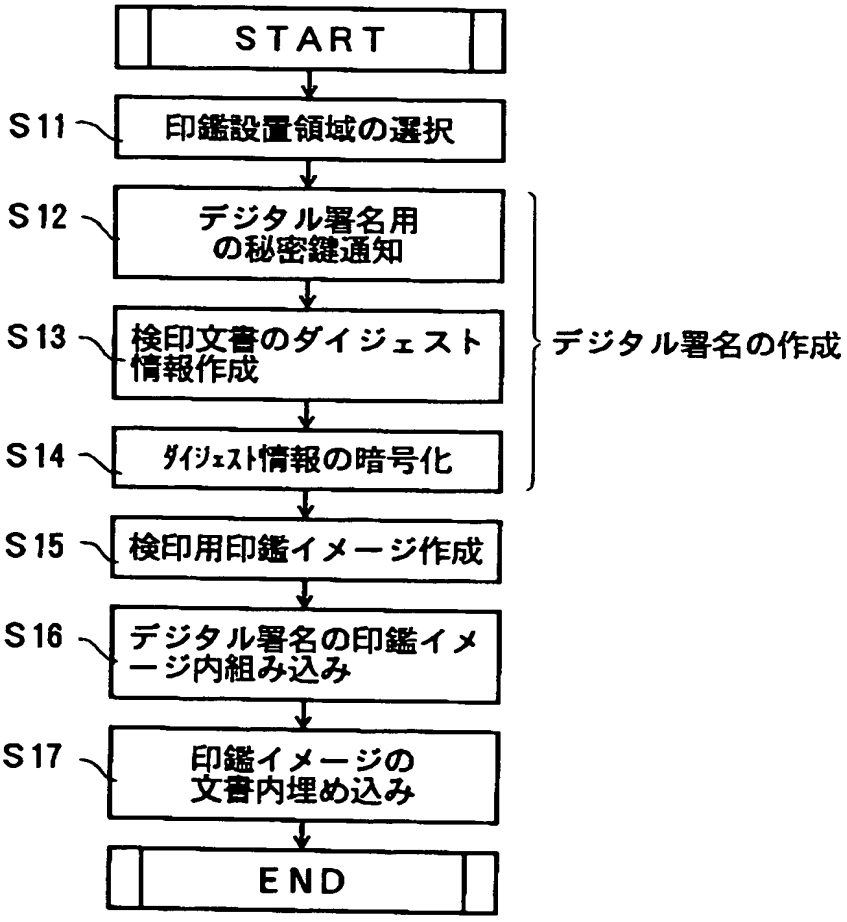
（B）



印鑑イメージの登録画面

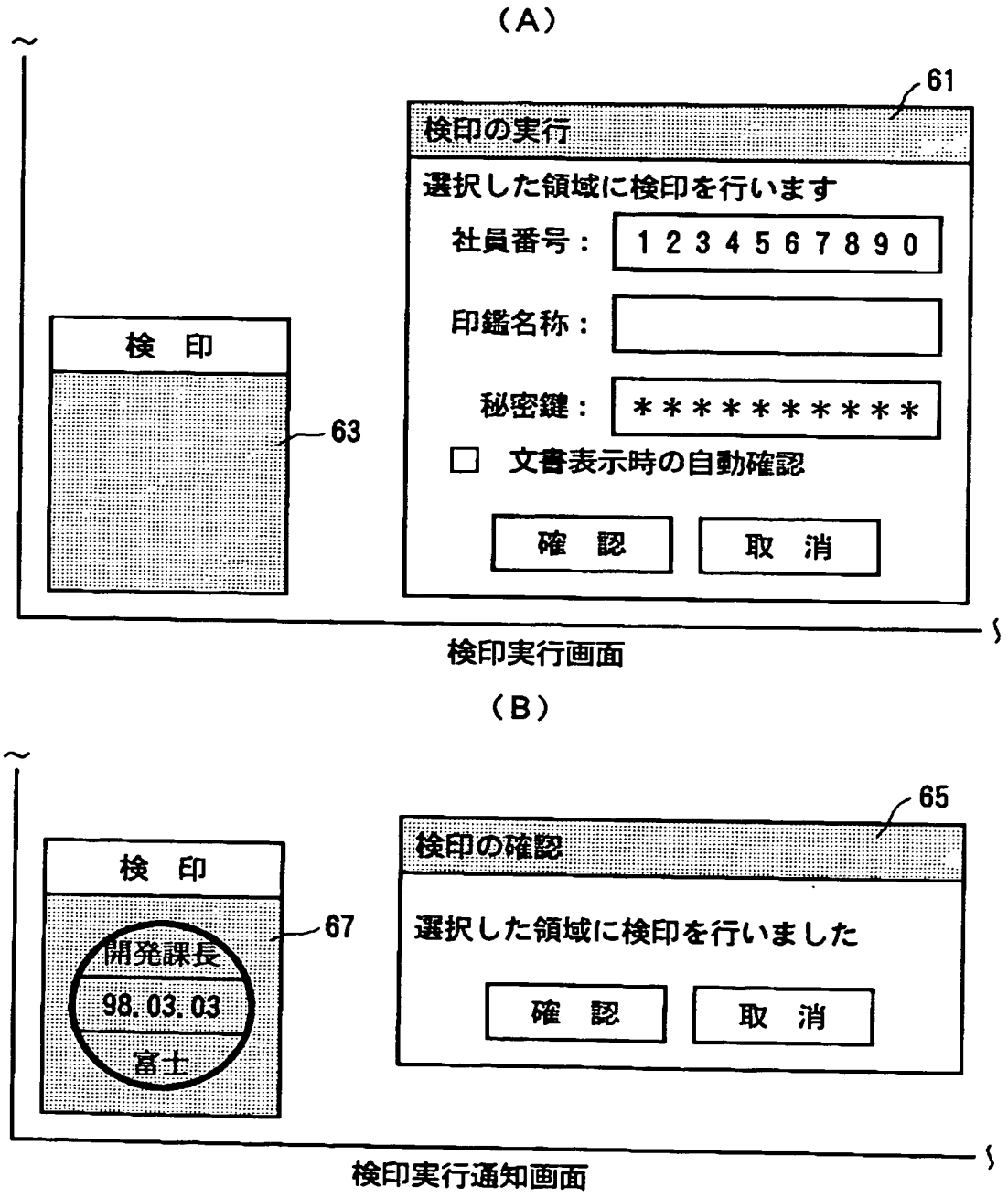
【図５】

検印の実行処理を説明するフローチャート図



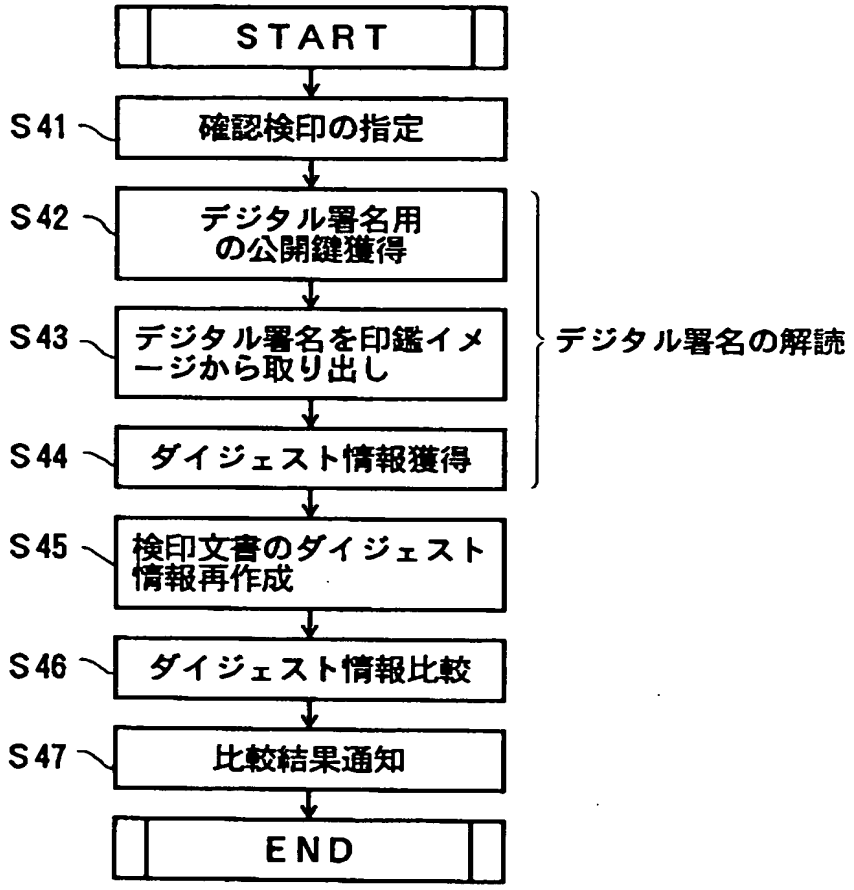
【図６】

検印を実行する画面の例を示す図



【図７】

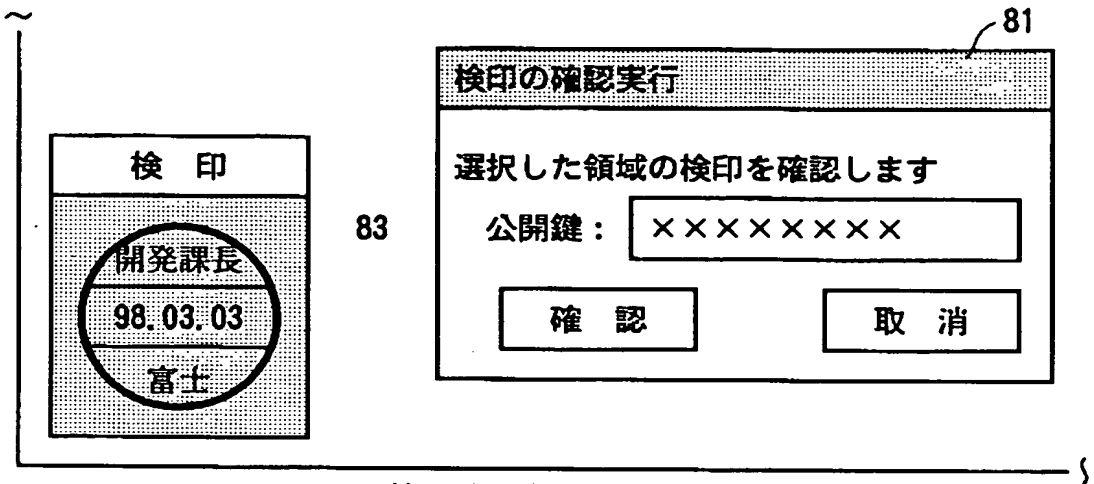
印鑑イメージの検証処理を説明するフローチャート図



【図８】

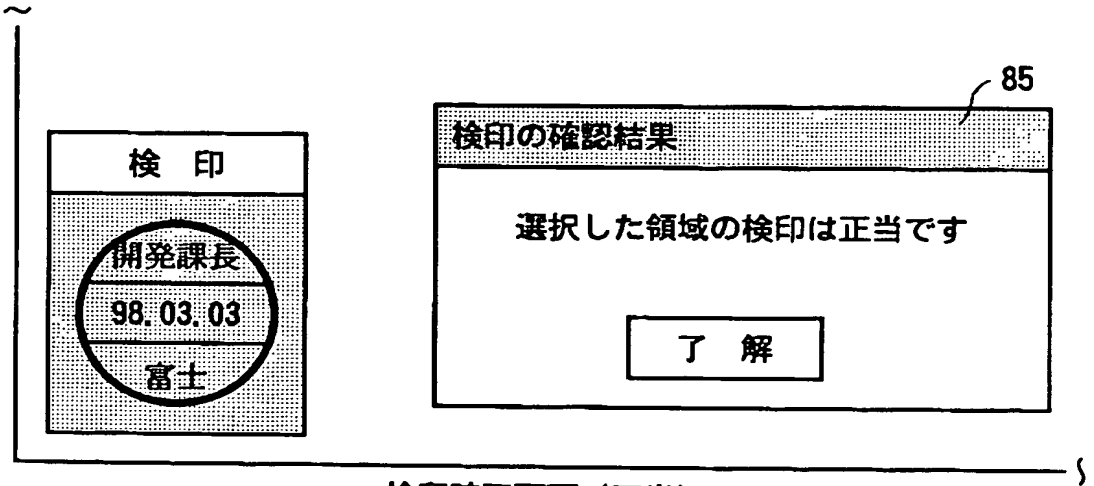
検印の確認する画面の例を示す図

（A）



検印確認実行画面

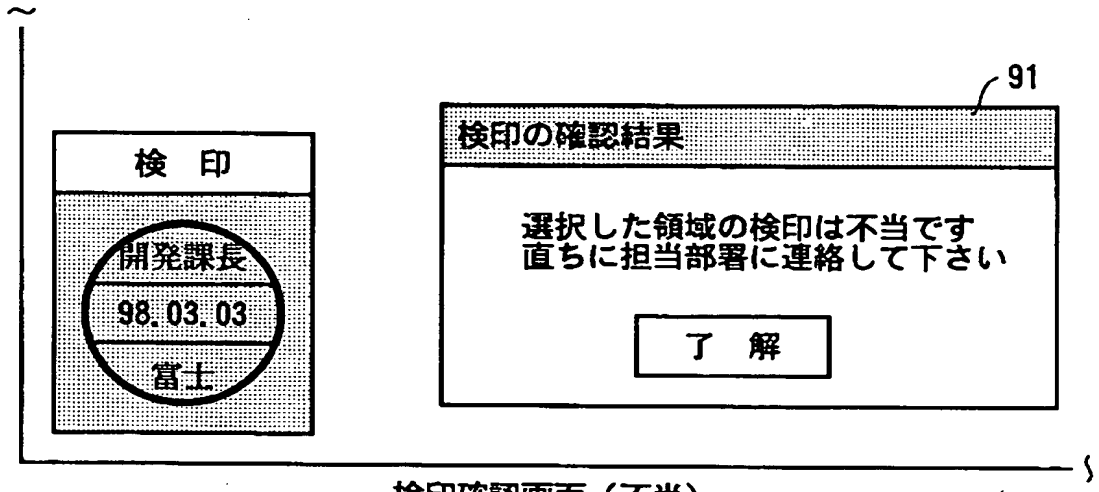
（B）



検印確認画面（正当）

【図９】

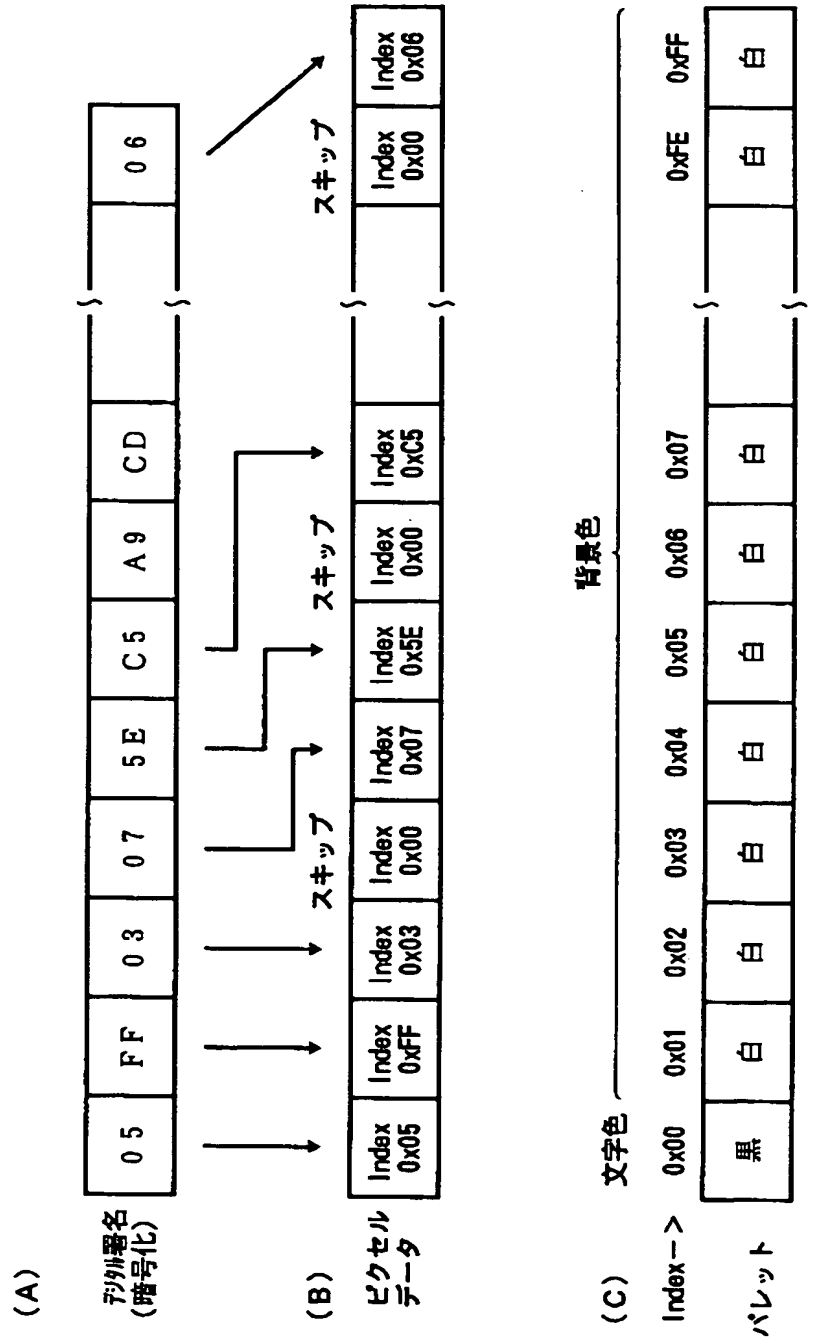
検印の確認する画面の例を示す図



検印確認画面（不当）

【図１０】

デジタル署名のイメージ組み込み説明図



【書類名】　　要約書

【要約】

【課題】　本発明の課題は、デジタル文章の認証に用いるランダムな数又は文字の列からなるデジタル署名を署名者の署名マークと共にイメージ情報に組み込むことにより視認性を向上するようにした認証装置を提供することを目的とする。

【解決手段】　本発明の課題は、デジタル署名を認証する認証装置において、署名者が設定した秘密鍵とデジタル文書の改ざんをチェックするダイジェスト情報とで暗号化してデジタル署名を生成する署名生成手段と、該デジタル署名と所定のマークとを合成したイメージ情報を作成する署名組み込み手段と、該署名組み込み手段で作成されたイメージ情報を、該デジタル文書内の指定された位置に埋め込むイメージ埋め込み手段とを有する認証装置にて達成される。

【選択図】　　図５

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社